Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

5 April 1983

MEMORANDUM FOR THE RECORD

SUBJECT: OSO Communications Upgrade Program (S)

1. Pursuant to a request by DDS&T/OSO, the manuals and documents relating to their impending Communications Upgrade Program (CUP) have been reviewed. The intention of the CUP is to replace the existing Remote Data Terminal, which was designed by OC, with a new data and message switching computer system. Several recommendations were made to [redacted] subsequent to the review. The purpose of this Memorandum for the Record is to document those recommendations. (S) 25X1

2. In the draft documents prepared by the contractor which were reviewed, computer security had not been adequately addressed. Therefore, it was recommended that the system security features and acceptance testing be based on the specifications of a B3 Trusted Computing Base (TCB) as contained in the Department of Defense Trusted Computer Evaluations Criteria (Final Draft, 27 January 1983), with the exception of those items dealing with mathematical modeling. Also provided to [redacted] was a list of some of the computer security features which were recommended for other communications computer switching systems. Attached to this memorandum is a list of those features. (S) 25X1

3. Although the primary objective was to review the project from a COMSEC point of view, several other recommendations were made as a result of the discussions with OSO. First, the project would benefit if an OC programmer were assigned full time to the project to work with the contractor and provide an insight into communications requirements and methodology. Second, COMSEC should continue to work closely with the project office to ensure the system adheres to good communications and computer security practices. Lastly, the Concept document contains a number of errors which indicate that the contractor does not have a firm grasp of communications requirements, formats, and procedures. (S)

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

[redacted]

Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

SUBJECT: OSO Communications Upgrade Program (S)

4. With regard to this last point, several personal recommendations were offered. Approximately three pages of notes relating to the Concept document and which dealt with communications computer design features, and operational matters and procedures were given to [redacted] However, prior to passing the notes it was explained that they were personal suggestions and they should not be considered official CSD recommendations since they did not deal directly with COMSEC matters. (C)

25X1

25X1 [redacted]

Attachment:
As stated

cc: DDS&T/OSO/CSS

Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

Attachment to OSO Communications Upgrade Program (S)

Security Considerations for Computer Systems

The system should incorporate sufficient checks so as to prevent the compromise of classified information, to insure the integrity of all information and software within the system, and to prevent the unauthorized or inadvertent modification of the system software. (C)

Memory Integrity

Techniques should be employed which will accurately and reliably ensure the integrity of the documents and data stored in memory. Sufficient checks shall be employed to prevent the transmission or manipulation of corrupted data. If a reliable and approved technique is not available, the operator should visually scan the outgoing data to ensure its integrity. (C)

Offline Mass Storage

A read/write scheme should be employed which will ensure the integrity of both software and data which is transferred to or from offline mass storage. Sufficient measures should be employed to ensure that the operator is immediately notified and system operation terminated whenever the integrity of data or software is in doubt. No software, which is read from disk, shall be executed if an error is detected during the read operation. (C)

Local User Authentication

Procedures should be employed which will accurately and reliably authenticate all local users who attempt to access the system. (C)

Remote System Identification

Prior to the transmission of any data to a remote system, the identity of the remote user must be established. This process may be performed manually or through the use of automated functions. (C)

25X1

Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

SECRET
Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1

Message Validation

Validation of all message formats which are processed by the system must be accomplished either manually or by the communications system. Areas of concern are: improper formatting of a message, inadvertent transmission of unvalidated messages, failure of any spill to operator instruction, and validation of message integrity (straggler protection). (C)

Audit Trails

The system must produce an audit trail (e.g. logs) containing sufficient information to permit a regular security review of the system. (C)

Degraded Operation

Any degraded mode of operation needs to include all security precautions and capabilities which are specified for normal operation. Whenever the system has degraded to the state under which the proper operation of the security features cannot be ensured, the system must be disabled and/or removed from service. (C)

Memory Buffers

All memory buffers/pages should be cleared subsequent to each use. (C)

SECRET
Approved For Release 2005/08/02 : CIA-RDP88-00893R000200040008-1